PCT WORLD INTELLECTUAL PROPER International Bur

INTERNATIONAL APPLICATION PUBLISHED UNDER ' WO 9606499A2

(51) International Patent Classification 6 : H04N

A2

(11) International Publication Number: WO 96/06499

(43) International Publication Date: 29 February 1996 (29.02.96)

(21) International Application Number: PCT/IB95/00601

(22) International Filing Date: 2 August 1995 (02.08.95)

(30) Priority Data:
9416040.5 9 August 1994 (09.08.94) GB

(71) Applicant: PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(71) Applicant *(for SE only)*: PHILIPS NORDEN AB [SE/SE]; Kottbygatan 5, Kista, S-16485 Stockholm (SE).

(71) Applicant *(for GB only)*: PHILIPS ELECTRONIS UK LIMITED [GB/GB]; 420-430 London Road, Croydon CR9 3QR (GB).

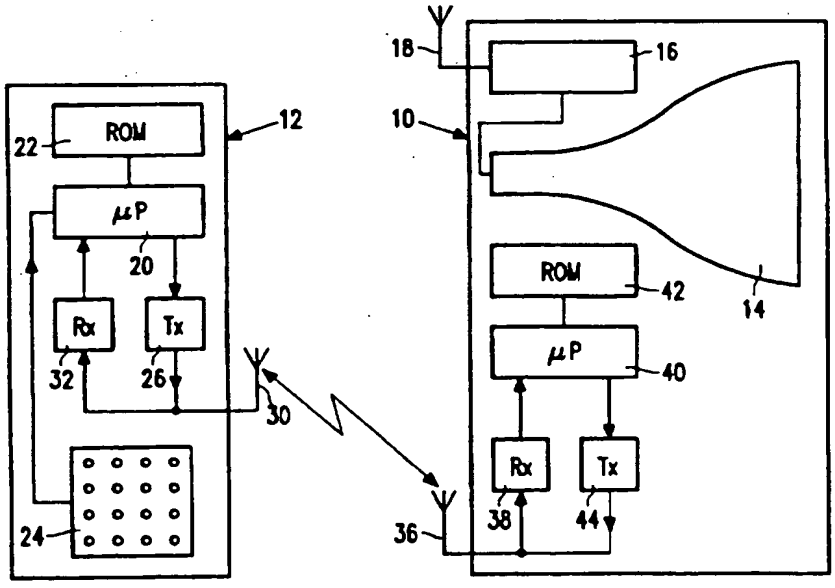
(72) Inventor: GIBSON, Rodney, William; Ferndale House, 66 Ferndale Road, Burgess Hill, Sussex (GB).

(74) Agent: MOODY, Colin, James; Internationaal Octrooibureau B.V., P.O. Box 220, 5600 AE Eindhoven (NL).

(81) Designated States: JP, KR, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD OF, AND SYSTEM FOR, TRANSFERRING SECURE DATA



(57) Abstract

A method of transferring secure data in a remote control system comprising a remote controller (12) and an apparatus (10) which is operable in response to commands relayed by way of the remote controller. The apparatus has a receiver (38) for receiving transmissions from the remote controller (12), the information from the said transmissions being stored in a storage device (42). The remote controller has a transmitter (26), a memory (22) for storing secure data and commands and a keypad (24). The transmitter (26) is controlled so that in response to a user wishing to transfer secure data to the user apparatus (10) it transmits this data at a power level lower than is normally used for sending other commans. The link between the remote controller (12) and the user apparatus (10) may be wireless or infra-red.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

DESCRIPTION

METHOD OF, AND SYSTEM FOR, TRANSFERRING SECURE DATA

Technical Field

The present invention relates to a method of, and system for, transferring secure data. The present invention has particular, but not exclusive, application to the use of a remote controller for controlling a user apparatus such as a TV receiver audio equipment and other items such as domestic appliances and/or office equipment.

Background Art

The use of infra-red remote controllers to control TV receivers and audio equipment is well known. A drawback which sometimes occurs in using infra-red controllers is that there is risk of cross-coupling, for example when a TV set remote controller sends commands to the TV receiver, which commands are picked up by other apparatus in the room causing it or them to be switched on unintentionally.

Remote controlled locking and unlocking of cars using infra-red radiation is well known, but has the disadvantage that a person equipped with what is termed "an electronic grabber" is able to detect the transmitted signal and to store it for unauthorised re-use later.

It is also known to use wireless remote controllers to operate remote apparatus having a radio receiver built into them, but drawbacks to such controllers are easy interception and the possibility of cross-coupling and spoofing, that is commands going to the wrong apparatus or being deliberately inserted by unauthorised parties. One method to avoid these problems is by the use of security coding, but this in turn gives a need to set up keys and authorisations. Such a task is not looked up as being a problem to technically adept people who may use PCs and be able to program video recorders, however entering such security data may represent a significant problem to unsophisticated users of electronic equipment.

Disclosure of Invention

An object of the present invention is to enter security data into a user apparatus in a simple but secure manner.

According to one aspect of the present invention there is provided a method of transferring secure data between a remote controller and an apparatus to be controlled by said controller, comprising positioning the remote controller and the apparatus close to each other and transferring the secure data at a power level lower than that normally used for transmitting commands by the remote controller.

According to a second aspect of the present invention there is provided a remote control system comprising a remote controller and an apparatus which is operable in response to commands relayed by way of the remote controller, the apparatus having means for receiving transmissions from the remote controller and storage means for storing secure data, and the remote controller having transmitting means, means for storing secure data and commands and a keypad, the transmitting means being responsive to the actuation of a key or combination of keys commanding the transfer of secure data, for transmitting said secure data at a power level lower than is used for sending other commands.

By means of the present invention a user can place a remote controller adjacent to and spaced from the user apparatus and by actuation of a key can transfer the data at a very low power. Since the power used to transmit the data is very low then it would be difficult for a "grabber" to detect the data being transferred. If desired communications between the remote controller and/or the user apparatus may be by way of radio or infra-red radiation.

Although the secure data, which may include security coding, may be held in the user apparatus or the remote controller, the security data being transmitted to the other device during the setting up procedure, an advantage for having it stored in the remote controller is that the same security data can be downloaded into several different pieces of apparatus.

If desired the remote controller may be used to link several pieces of apparatus in a secure manner by picking up data, for example sub-system

addresses, and transferring the data to one or more apparatus which are to be linked.

In some cases it may be desirable to ensure that an authorised person was operating the remote controller. In such an arrangement, a personal identity number (PIN) could be used to authorise the transaction. For extra security if the PIN is transmitted it may be encoded, using pre-set coding and/or a code set up at the commencement of the operation to transfer the secure data.

In order to increase the overall security of the device the security data may be encoded using a pseudo-random code which is automatically changed in a predetermined way so that the same information is never sent twice. The pseudo-random code in the apparatus is changed by the same algorithm as that used in the remote controller. As a result, an unauthorised person who is able to detect the transmissions cannot gain access by re-using the format of the information transmitted. The code keys and any other secret information used by these algorithms are transferred using the method in accordance with the present invention.

Brief Description of Drawings

The present invention will now be described, by way of example, with reference to the accompanying drawings, wherein:

Figure 1 is a block schematic diagram of a wireless remote controller and a TV receiver,

Figure 2 is simplified version of the drawing shown in Figure 1 wherein the remote controller is an infra-red remote controller and transmissions from the apparatus to the remote controller are also by way of infra-red radiation,

Figure 3 is a flow chart relating to the transmission of security data by low power, and

Figure 4 is a flow chart relating to recognising a new equipment.

In the drawings the same reference numerals have been used to indicate corresponding features.

Modes for Carrying Out the Invention

The arrangement shown in Figure 1 comprises a user apparatus in the form of a TV receiver 10 and a wireless remote controller 12. The TV receiver 10 comprises a display device such as a cathode ray tube 14 to which is connected the usual television receiver circuitry 16 which is known per se and forms no part of the present invention. As is customary the circuitry 16 is connected to an antenna 18.

The remote controller 12 comprises a microprocessor 20 to which is connected a read-only memory (ROM) 22 which stores security data such as coding. A keypad 24 is connected to the microprocessor 20 and serves as a man-machine interface. A radio transmitter 26 is provided and has an input connected to the microprocessor 20 and an output coupled to an antenna 30. A receiver 32, which may be optional, is connected between the antenna 30 and the microprocessor 20.

Inside the TV receiver 10, an antenna 36 is connected to a radio receiver 38 having an output connected to a microprocessor 40. A non-volatile ROM 42, for example an EPROM, is connected to the microprocessor 40 and serves to store security data relayed from the remote controller 12. Optionally a transmitter 44 is connected to an output of the microprocessor 40 and the antenna 36.

The frequency of operation of the transmitter 26 depends on that approved by the radio regulatory authorities but a frequency of the order of 400MHz is considered suitable. The transmitter 26 is able to operate in a very low power mode, of the order of microwatts or picowatts, when relaying security data from the remote controller 12 to the receiver 38. In order to do this, the remote controller has to be held close to the antenna 36 and separated by a space of, say, 10cm and by pressing a predetermined button or sequence of buttons on the remote controller 12, the remote controller transmits at low power to the receiver 38 to introduce itself. The information sent to the receiver 38 for ultimate storage in the ROM 42 includes an identity code and keys or algorithms for use as security codes in subsequent transactions at normal power. This operation could form an authorisation

process in which the TV receiver 10 becomes aware of the identity of the remote controller 12 and thereafter obeys its commands. An additional level of security can be provided by the remote controller storing a personal identity number (PIN) which can be used either to authorise transmission of secure data or as part of the transactions of not only transferring security data at low power but also in the normal channel changing and other adjustments that user may want to effect. In its most elementary form the remote controller 12 does not include the receiver 32 and likewise the TV receiver 10 does not include the transmitter 44. By omitting these items the signalling is essentially one way from the remote controller to the TV receiver. However, by including the receiver 32 and the transmitter 44 information may be exchanged between the remote controller and the TV receiver and/or other equipment which are to be linked, for example acknowledgements may be provided to transmissions originating from the remote controller. Such acknowledgements will also conform to the protocol applying so that transmissions at the normal, higher, power do not reveal unwanted information which can be used by an unauthorised third party or another interfering apparatus. In the case of linking equipments, the remote controller 12 is able to pick-up secure data from one piece of apparatus and transfer the data at low power to one or more other pieces of apparatus, for example to link sub-system addresses in a secure manner.

Figure 2 is a simplified version of Figure 1 and illustrates that communication between the remote controller 12 and the TV receiver 10 is via an infra-red link, the remote controller 12 having an infra-red emitter 50 and the TV receiver an infra-red detector 52. In order to be able to provide linking facilities and/or acknowledgements the TV receiver 10 further comprises an infra-red emitter 54 and the remote controller an infra-red detector 56. A disadvantage of using infra-red transmissions over and above wireless transmissions is that the detector 52 and emitter 54 have to be disposed on the front of the TV receiver 10 whereas in the Figure 1 arrangement the antenna 36 can be placed at the rear of the apparatus and the associated circuitry located in the relatively large space surrounding the

neck of the display tube 14.

Figure 3 is a flow chart relating to the sequence of operations associated with transmitting secure data at low power from a remote controller programmed with a PIN. The flow chart commences with a terminator block 60. The block 62 relates to actuating the keypad of the remote controller to key in inputs for transferring data. The block 64 relates to the microprocessor 20 (Figure 1) recognising the commands in the data being transferred. Block 66 relates to checking to see if the command relates to the transfer of secure data. If the answer is No (N) then the required data is transmitted by the remote controller at normal power. This is indicated by block 68. If the answer to block 66 is Yes (Y) then in block 70 the question is asked "Is a PIN required?". If the answer is Yes (Y) then block 72 relates to a user entering his PIN and in block 74 a check is made to see if the PIN is recognised. If the answer is No (N) then the flow chart reverts to the block 62. Alternatively, if the answer is Yes (Y), then the flow chart proceeds to the block 76 which also is connected to the No (N) output of the block 70. The block 76 relates to transmitting secure data and, optionally the PIN, at low power.

Although an in-range detector may be provided, a more elementary way of checking that the data has been transferred is to send a normal power command and see if the TV receiver (or other user equipment) responds as required. In the event of the secure data not having been received then the user re-tries with the remote controller positioned closer to the antenna or detector of the receiving equipment.

Figure 4 relates to a flow chart in respect of a user equipment such as the TV receiver 10 (Figure 1) receiving low power transmissions from a remote controller and having the ability to respond to enquiries made by the remote controller. Block 82 refers to switching the TV receiver on. Block 84 relates to the equipment responding by transmitting the equipment details which may include a code identifying the manufacturer, the type of equipment, for example TV receiver, hi-fi equipment, and a type number. In block 86 the TV receiver receives the system identification code, which

ensures that the transmission was intended for the TV receiver, transmitted by the remote controller which is followed by receiving additional secure data such as security coding, algorithms and so forth, block 88. Block 90 refers to storing the secure data, for example in the ROM 42 (Figure 1). Finally, block 92 relates to the TV receiver waiting to receive commands at normal power level from the remote controller.

By means of the present invention one remote controller can be used to operate several pieces of equipment which form parts of a home system network or in an office environment. Additionally, by means of the creation of a network of equipment and the use of security coding, equipment can "talk" to each other without additional commands from the remote controller.

Although the present invention envisages a wireless or infra-red link between the remote controller and the user apparatus, other known forms of communication, such as ultrasonics, or ohmic contact may be used for the transfer of secure information. In the case of using ohmic contact then either a special connector can be provided between the remote controller and the user apparatus or the user apparatus has a storage compartment for receiving the remote controller, the storage compartment and the remote controller having complementary electrical contacts which mate when the remote controller is inserted into the storage compartment.

From reading the present disclosure, other variations and modifications will be apparent to persons skilled in the art. Such variations and modifications may involve equivalent and other features which are already known in the design, manufacture and use of remote control systems and component parts thereof, and which may be used instead of or in addition to features already described herein. Although claims have been formulated in this Application to particular combinations of features, it should be understood that the scope of the disclosure of the present invention also includes any novel feature or any novel combination of features disclosed herein either explicitly or implicitly or any generalisation thereof, whether or not it relates to the same invention as presently claimed in any claim and whether or not it mitigates any or all of the same technical problems as does the present

invention. The Applicants hereby give notice that new claims may be formulated to such features and/or combinations of such features during the prosecution of the present Application or of any further Application derived therefrom.

Industrial Applicability

Remote control of equipment or groups of equipments.

CLAIMS

1. A method of transferring secure data between a remote controller and an apparatus to be controlled by said controller, comprising positioning the remote controller and the apparatus close to each other and transferring the secure data at a power level lower than that normally used for transmitting commands by the remote controller.

2. A method as claimed in claim 1, characterised in that the secure data comprises an algorithm for changing the code which is transmitted as part of a command.

3. A method as claimed in claim 1 or 2, characterised in that the secure data is transferred by radio.

4. A method as claimed in any one of claims 1 to 3, characterised in that the secure data is held by the remote controller, in that a personal identification number (PIN) is assigned to the remote controller and in that the PIN is used to authorise the transaction for transferring the secure data.

5. A method as claimed in claim 4, characterised in that the apparatus communicates with the remote controller by the same type of link as is used to transfer the secure data.

6. A method as claimed in claim 5, characterised in that the remote controller is able to receive data from one piece of apparatus and able to transfer the said data to at least one other piece of apparatus.

7. A remote control system comprising a remote controller and an apparatus which is operable in response to commands relayed by way of the remote controller, the apparatus having means for receiving transmissions from the remote controller and storage means for storing secure data, and

the remote controller having transmitting means, means for storing secure data and commands and a keypad, the transmitting means being responsive to the actuation of a key or combination of keys for commanding the transfer of secure data, for transmitting said secure data at a power level lower than is normally used for sending other commands.

8. A system as claimed in claim 7, characterised in that the transmitting and receiving means are radio transmitting and receiving means.

9. A system as claimed in claim 7 or 8, characterised in that the remote controller has means for storing a PIN number and the apparatus has means for storing the PIN number when received as part of the transaction for transferring the secure data.

10. A system as claimed in claim 7, 8 or 9, characterised in that the apparatus comprises transmitting means and the remote controller comprises receiving means, whereby data can be communicated to the remote controller by the apparatus.

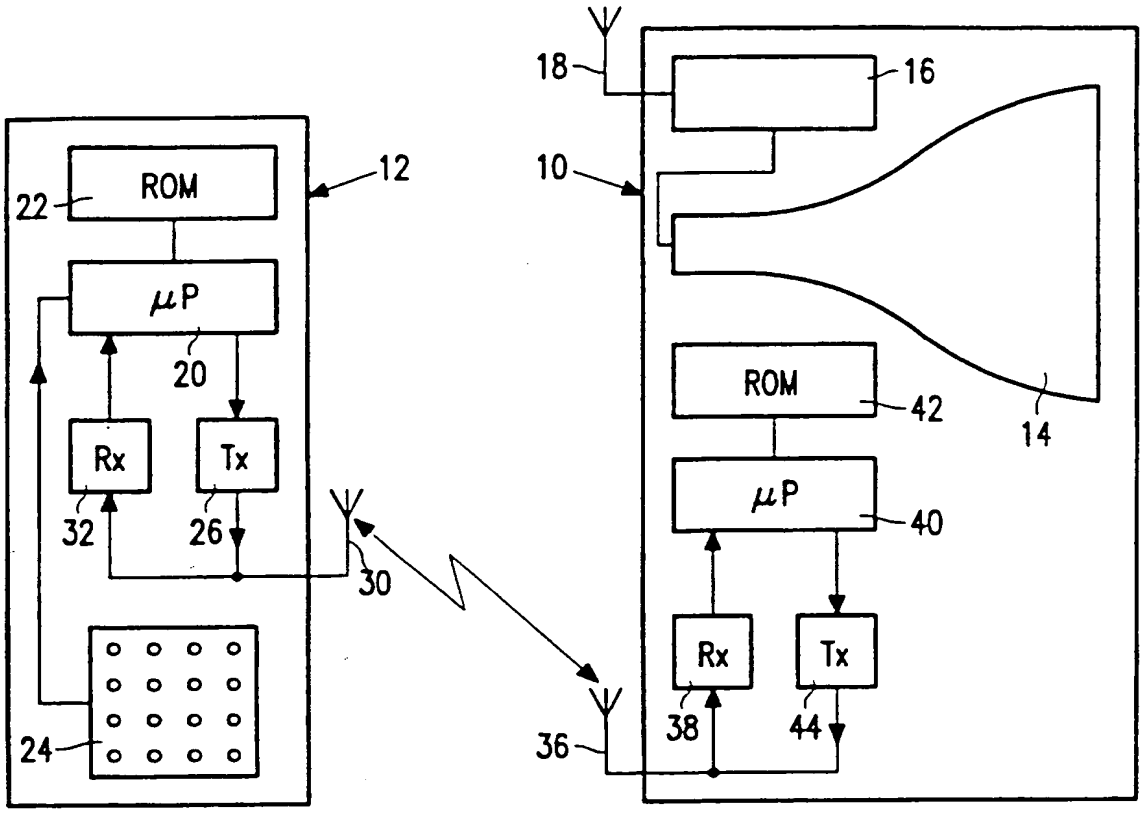

18
16
10
12
22
ROM
μP
20
Rx
Tx
32
26
30
24
ROM
42
14
μP
40
Rx
Tx
38
44
36

FIG. 1

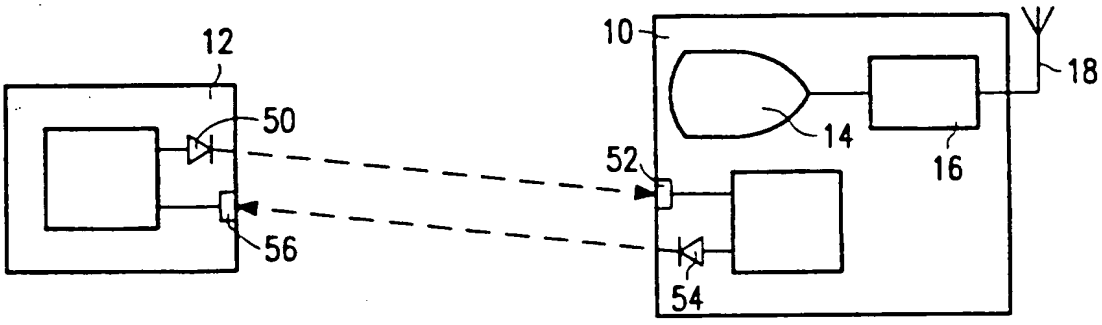

12
50
56
10
18
14
16
52
54

FIG. 2

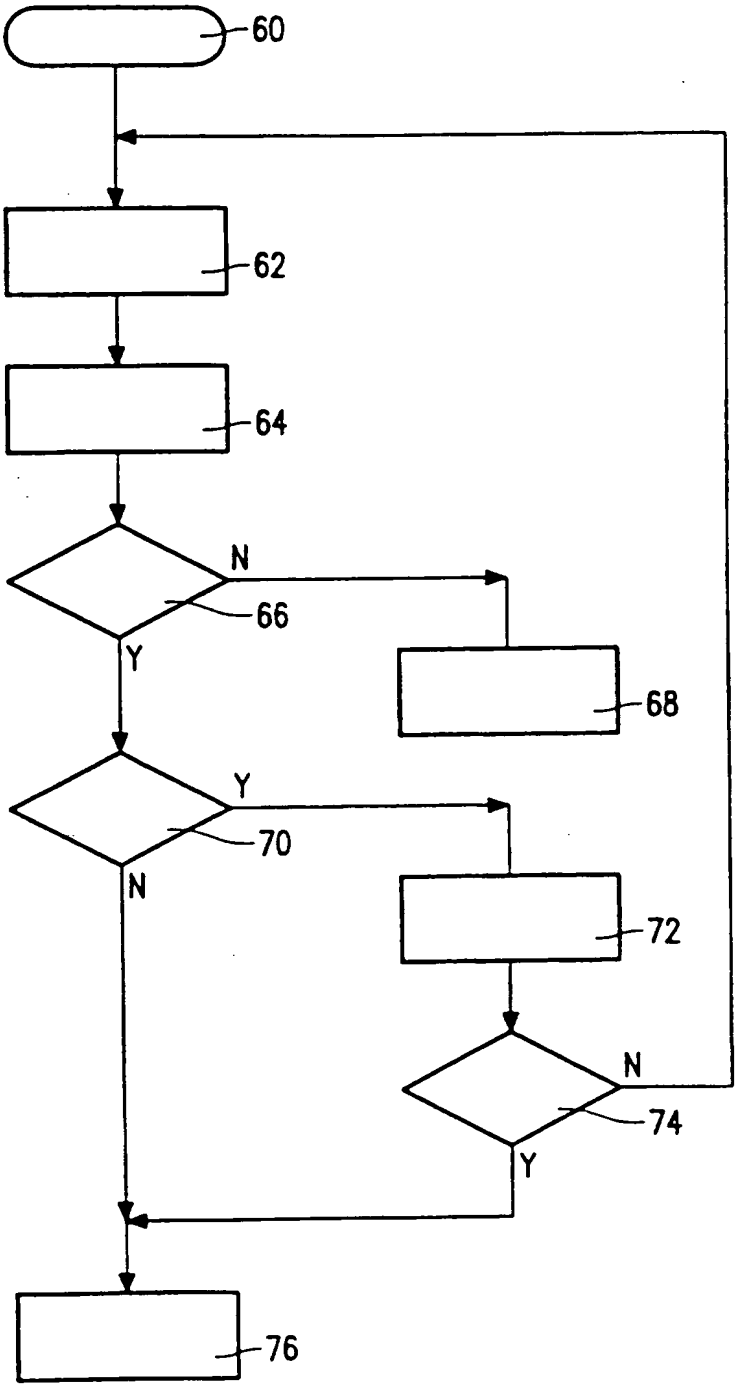


FIG. 3

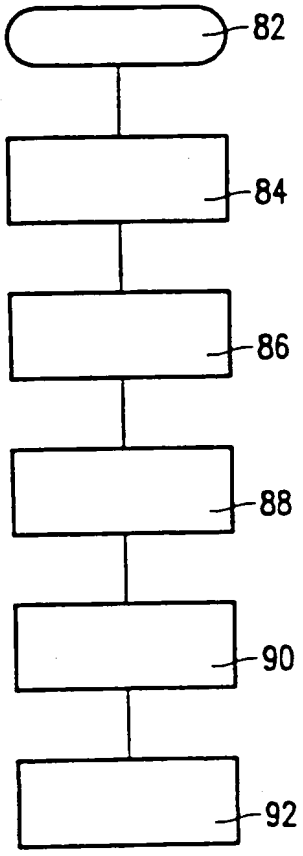


FIG. 4

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classificati n 6 : **H04B 1/034, 1/20, E05B 49/00** — **A3**

(11) International Publication Number: **WO 96/06499**

(43) International Publication Date: 29 February 1996 (29.02.96)

(21) International Application Number: PCT/IB95/00601

(22) International Filing Date: 2 August 1995 (02.08.95)

(30) Priority Data:
9416040.5 9 August 1994 (09.08.94) GB

(71) Applicant: PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(71) Applicant *(for SE only)*: PHILIPS NORDEN AB [SE/SE]; Kottbygatan 5, Kista, S-16485 Stockholm (SE).

(71) Applicant *(for GB only)*: PHILIPS ELECTRONIS UK LIMITED [GB/GB]; 420-430 London Road, Croydon CR9 3QR (GB).

(72) Inventor: GIBSON, Rodney, William; Ferndale House, 66 Ferndale Road, Burgess Hill, Sussex (GB).

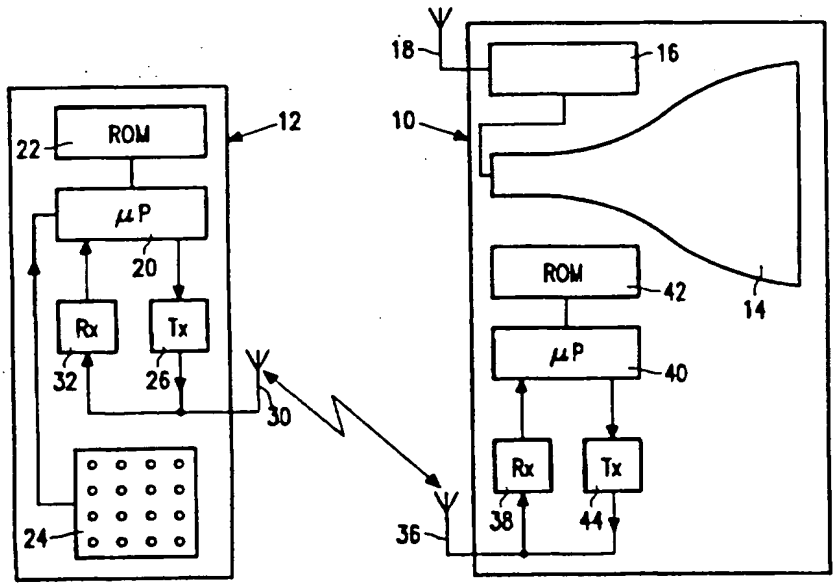
(74) Agent: MOODY, Colin, James; Internationaal Octrooibureau B.V., P.O. Box 220, 5600 AE Eindhoven (NL).

(81) Designated States: JP, KR, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
11 April 1996 (11.04.1996)

(54) Title: METHOD OF, AND SYSTEM FOR, TRANSFERRING SECURE DATA



(57) Abstract

A method of transferring secure data in a remote control system comprising a remote controller (12) and an apparatus (10) which is operable in response to commands relayed by way of the remote controller. The apparatus has a receiver (38) for receiving transmissions from the remote controller (12), the information from the said transmissions being stored in a storage device (42). The remote controller has a transmitter (26), a memory (22) for storing secure data and commands and a keypad (24). The transmitter (26) is controlled so that in response to a user wishing to transfer secure data to the user apparatus (10) it transmits this data at a power level lower than is normally used for sending other commans. The link between the remote controller (12) and the user apparatus (10) may be wireless or infra-red.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 95/00601

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04B 1/034, H04B 1/20, E05B 49/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04B, E05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, CLAIMS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4881148 A (G. LAMBROPOULOS ET AL.), 14 November 1989 (14.11.89), column 4, line 5 - line 8; column 17, line 7 - line 9, figure 5A, claim 1, abstract	1-3,7,8,10
A	--	4-6,9
Y	EP 0524424 A1 (MERCEDES-BENZ AG), 27 January 1993 (27.01.93), figures 4,5, abstract	1-3,7,8,10
	--	
Y	US 5148159 A (J. CLARK ET AL.), 15 Sept 1992 (15.09.92), figure 1, abstract	1,7,10
A	--	2-6,8,9

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 February 1996	15 -02- 1996
Name and mailing address of the ISA/ Swedish Patent Office, Box 5055, S-102 42 STOCKHOLM, Facsimile No. +46 8 666 02 86	Authorized officer: Harriet Ekdahl, Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 95/00601

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim N
Y	EP 0385070 A1 (DAIMLER-BENZ AKTIENGESELLSCHAFT), 5 Sept 1990 (05.09.90), figure 1, claim 1, abstract	2
A	--	1,3-10
A	EP 0320439 A2 (REMOTE AUTOMATION & CONTROL ELECTRONICS INC.), 14 June 1989 (14.06.89), figure 1, claim 1, abstract	1-10
	--	
A	EP 0244332 A1 (SOUM, RENE), 4 November 1987 (04.11.87), claim 5	1-10
	--	

INTERNATIONAL SEARCH REPORT

Information on patent family members

05/01/96

International application No.
PCT/IB 95/00601

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A- 4881148	14/11/89	EP-A,A,A 0292217	23/11/88
		JP-B- 7091913	09/10/95
		JP-A- 63308171	15/12/88
		US-A- 5109221	28/04/92
		US-A- 5252966	12/10/93
		US-A- 5406274	11/04/95
EP-A1- 0524424	27/01/93	DE-A- 4124181	21/01/93
		JP-A- 5206874	13/08/93
		US-A- 5355525	11/10/94
US-A- 5148159	15/09/92	NONE	
EP-A1- 0385070	05/09/90	SE-T3- 0385070	
		DE-A,C- 3905651	30/08/90
		ES-T- 2051390	16/06/94
		JP-A- 2250497	08/10/90
		US-A- 5159329	27/10/92
EP-A2- 0320439	14/06/89	CA-A- 1252545	11/04/89
		JP-A- 2048897	19/02/90
		US-A- 4928778	29/05/90
EP-A1- 0244332	04/11/87	FR-A,B- 2597538	23/10/87
		US-A- 5107258	21/04/92